



IT NATION™

SECURE

hosted by  CONNECTWISE

# Cyber Insurance and MSP: Caught in the Crossfire

Presented by: Wes Spencer VP, Cybersecurity Strategy, CyberFOX



IT NATION™ **SECURE**

# Wes Spencer

## Professional:

- Based in Tampa, FL
- VP, Cybersecurity Strategy, CyberFOX
- Board Advisor, FifthWall Solutions
- Founder, CEO Empath Cyber
- Cybersecurity expert and co-founder of Perch Security
- Former (recovering) bankster – CIO at FNB Bank
- Chairman of FS-ISAC CIC – Cyber threat sharing group of 4,000+ banks and credit unions
- 2020 National Cybersecurity Educator of the Year

## Personal:

- I run a YouTube channel of 80k subs on cybersecurity + crypto + startups
- Super duper into bourbon and cryptocurrency (not at the same time)
- I play too much Minecraft with the kids



# Right from the ancient manuscripts

"Most security-related training courses and documentation discuss the implementation of a principle of least privilege, **yet organizations rarely follow it**. The **principle is simple**, and the impact of applying it correctly **greatly increases your security and reduces your risk**. The principle states that all users should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more."

[The Administrator Accounts Security Planning Guide, 1999](#)



# WHO WE ARE

---



**FIFTHWALL**  
S O L U T I O N S  
CYBER INSURANCE SIMPLIFIED

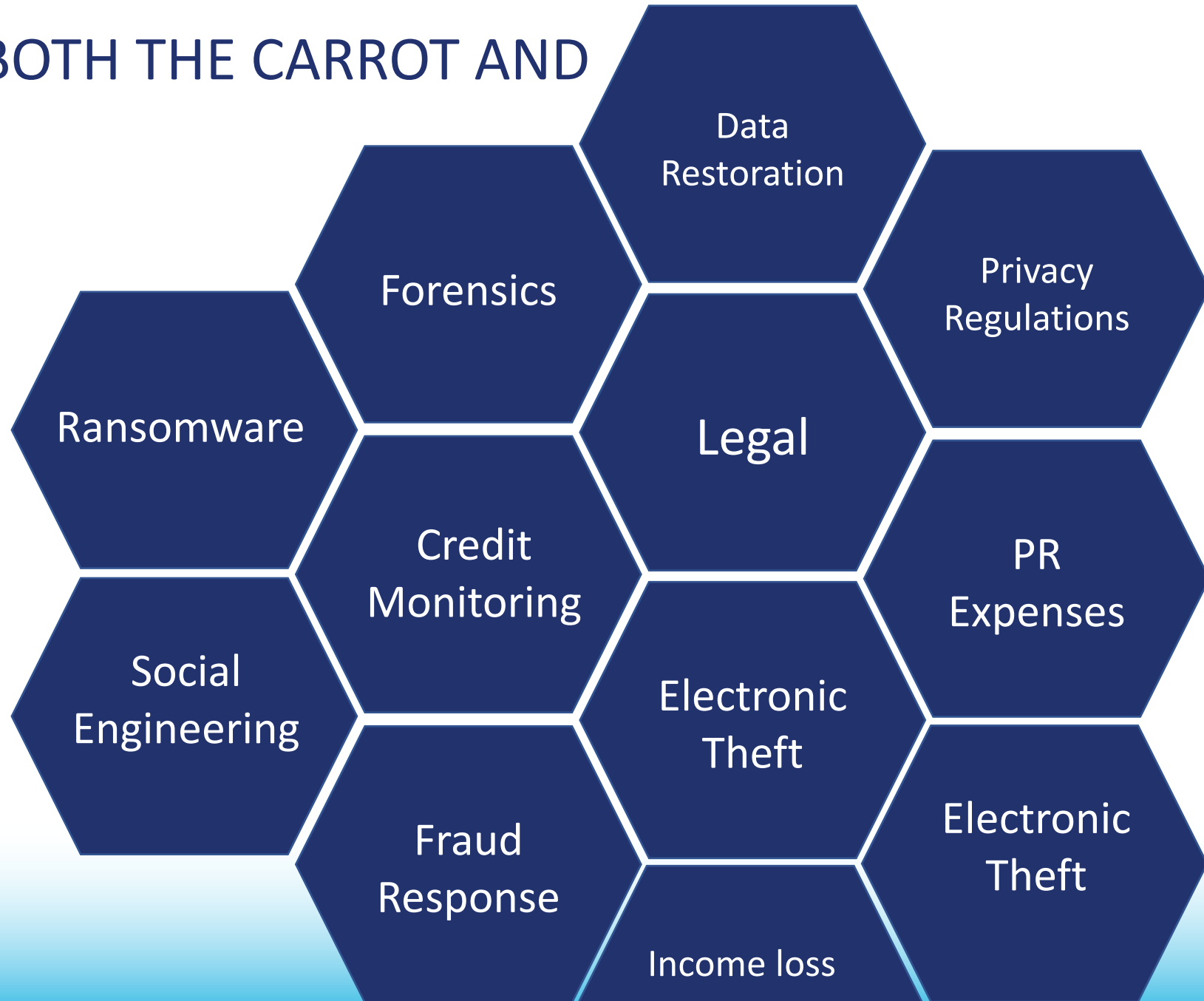
- Distributor of cyber insurance
- Direct contact with 40+ carriers
- Largest & Oldest (2016), 100% cyber focused
- 1,000+ agencies work with us
- Built for MSPs
- 600+ MSP Elite Partners
  - And counting!

# WHO WE ARE

- We are a **wholesaler** (think of us as a **distributor**) with **over 35 years experience** – we have **near global access to all cyber insurance** products in the marketplace.
- We are also an **MGU** (think of us like a **carrier**) – We have our own insurance policies that we customize, design and bring to market.
  - **Full control** over the application process, pricing, security requirements, etc.
  - **Authority** to provide **discounts** based on certain security controls and products –
    - FW has **full control** over the IR/claims process

# CYBER INSURANCE IS BOTH THE CARROT AND THE STICK

- It's Comprehensive
- It includes coverage for IR
- It includes critical crime coverages. (e.g. Ransomware)
- It's NOT compliance focused
- It's not attached to other lines of coverage (endorsements)



# WHAT IS TECH E&O?

- It's an **additional** coverage for Tech Service type businesses
- **MSPs** need/want this coverage.
- It provides liability coverage for the services an MSP provides to their clients.
- **Many carriers are steering away from providing this coverage for MSP's.**



# HOW DID WE GET HERE?

2015 - 2018

- Cyber insurance was low cost with very little underwriting.
- **Adoption was low** (around 10%) but the process was very simple and easy

2019

- Claims started rising significantly!
- Awareness and defenses are still low.
- Ransomware was hot on the scene - carriers were **NOT** prepared

2020

- Incidents still rising, and the pandemic forced work from home shift.
- Demand for cyber insurance skyrocketed and carriers are losing money rapidly.
- **Underwriting actually starts getting serious**

2022-23

- Incident volume is slowing down (largely due to conflict in Ukraine)
- More minimum standards required for cybersecurity controls
- **New focus on continuous underwriting**



# OPRAH SAID IT



# WE READ ABOUT IT

## THE WALL STREET JOURNAL.

Subscribe | Sign In

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work Style Sports

Search 

SHARE



PRO CYBER NEWS

### Cyber Insurers Raise Rates Amid a Surge in Costly Hacks

Insurance market resets after a ransomware boom and the threat of spillover from Ukraine



#### MOST POPULAR NEWS

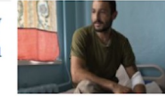
1. These Workers Were the Bosses' Favorites. Now They Feel Jilted.



2. This Men's Pants Style Is Back—and For All Ages



3. Ukrainian Soldiers Say They Are Advancing in the South, but at a Cost



4. As the U.S. Dollar Surges, American Buyers Splurge on European Homes



5. Sarah Palin Loses Alaska House Race to Mary Peltola



#### MOST POPULAR OPINION

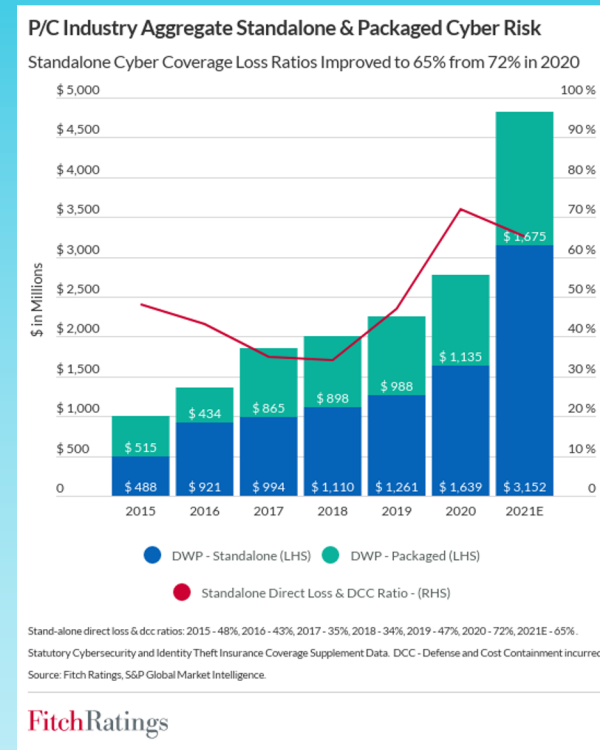
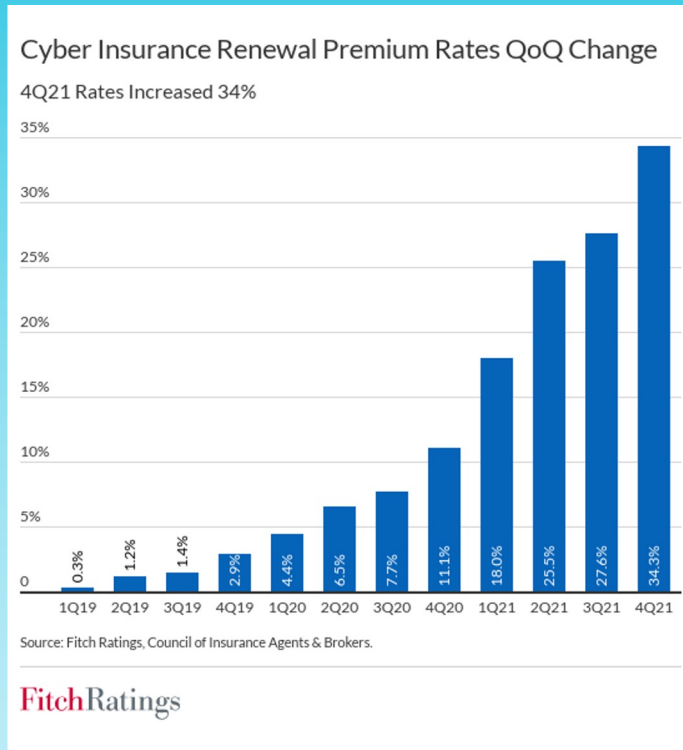
1. Opinion: Donald



#ITNa

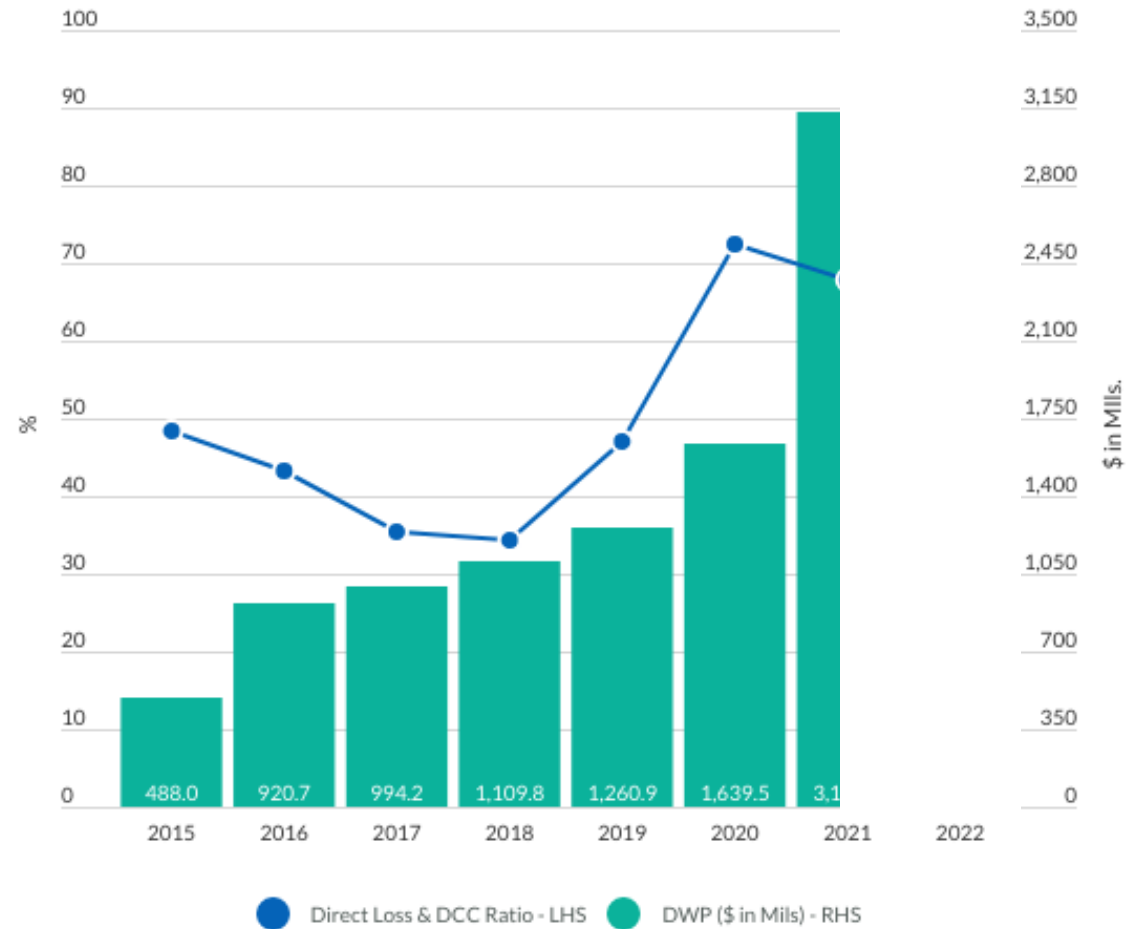
ON

# WHAT THE DATA SHOWS



## Standalone Cyber Risk Direct Loss & DCC Ratios

The Combined Ratio Improved 25 Percentage Points in 2022 Amid a 62% Increase in Premiums



PC Industry Aggregate. LHS - left-hand side axis. RHS - right-hand side axis. DCC - Defense and Cost Containment incurred. DWP - Direct written premium. Note: Statutory Cybersecurity and Identity Theft Insurance Coverage Supplement Data.

Source: Fitch Ratings, S&P Global Market Intelligence

FitchRatings





**Meredith Schnur** · 2nd

Managing Director, US and Canada Cyber Brokerage Leader at Marsh USA, Inc.

“The US cyber insurance market **continues to stabilize**. Barring unforeseen events, we expect to see continued **deceleration of rate increases** for the remainder of 2023, especially for organizations with good cyber hygiene and loss histories.”







# All is not rainbows and unicorns

- Frequency of ransomware has returned following a brief lull last year compared to 2021.
- Ransomware-related claims rose 77% in the first quarter compared to Q4 2022.
- Privacy-related claims are up 85% over the last quarter of 2022.

# So here's the latest for MSPs...

- Your controls are working
- Carriers are seeing way less "direct events" like ransomware and business email compromise
- The majority of Tech E&O is from MSPs making mistakes:
  - Loss of data
  - Less cyber crime and more mistakes being made

# high risk industries (from a carrier perspective)

- Municipalities
- Payment Processors
- Schools & Colleges
- Healthcare institutions
- Small businesses
- Law Firms
- Engineering
- Manufacturing
- Crypto and pr0n
- IT companies (meaning you)

# WE READ ABOUT IT

MYNEWMARKETS.COM | CLAIMS JOURNAL | INSURANCE JOURNAL TV | ACADEMY OF INSURANCE | CARRIER MANAGEMENT


## INSURANCE JOURNAL

**Featured Stories**

- Florida's Citizens Tops 1 Million Policies
- Tennessee Launches Captive Cyber, Property Insurer

News | Markets

**Current Magazine**




Read Online

Subscribe





Front Page ▾ | News ▾ | Magazines ▾ | Research | Directories | Jobs | Features ▾ | Subscribe

### Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use

By Chad Hemenway | July 12, 2022





✉ Email This | 📧 Subscribe to Newsletter



# WE READ ABOUT IT


SIGN IN **The Register**  


{\* CSO \*}

## PC store told it can't claim full cyber-crime insurance after social-engineering attack

Two different kinds of fraud, says judge while throwing out lawsuit against insurer

Brandon Vigliarolo Tue 16 Aug 2022 // 16:43 UTC

4 



A Minnesota computer store suing its crime insurance provider has had its case dismissed, with the courts saying it was a clear instance of social engineering, a crime for which the insurer was only liable to cover a fraction of total losses.

SJ Computers alleged in a [November lawsuit](#) [PDF] that Travelers Casualty and Surety Co. owed it far more than paid on a claim for nearly \$600,000 in losses due to a successful [business email compromise](#) (BEC) attack.

According to its website, SJ Computers is a Microsoft Authorized Refurbisher, reselling Dell, HP, Lenovo and Acer products, as well as providing tech services including software installs and upgrades.

Travelers, which filed a motion to dismiss, said SJ's policy clearly delineated between computer fraud and social engineering fraud. The motion was [granted](#) [PDF] with prejudice last Friday.

In the dismissal order, the US District Court for Minnesota found that the two policy agreements are mutually exclusive, as well as finding SJ's claim fell squarely into its social engineering fraud agreement with Travelers, which has a cap of \$100,000.

When SJ filed its claim with Travelers, the court noted, it did so only under the social engineering fraud agreement. After realizing the policy limit on computer fraud was 10 times higher, "SJ Computers then made a series of

# CYBER INSURANCE IS KNEE JERK





# ASSUME BREACH

When not if – you need coverage

“Nobody is stopping the most elite attacks” ...**but we can raise the bar / minimize the blast radius against the majority of attacks, especially financially motivated ones**

Forensics, legal, etc to *legally* protect your business.

Technical aspect is a small portion.

#ITNation

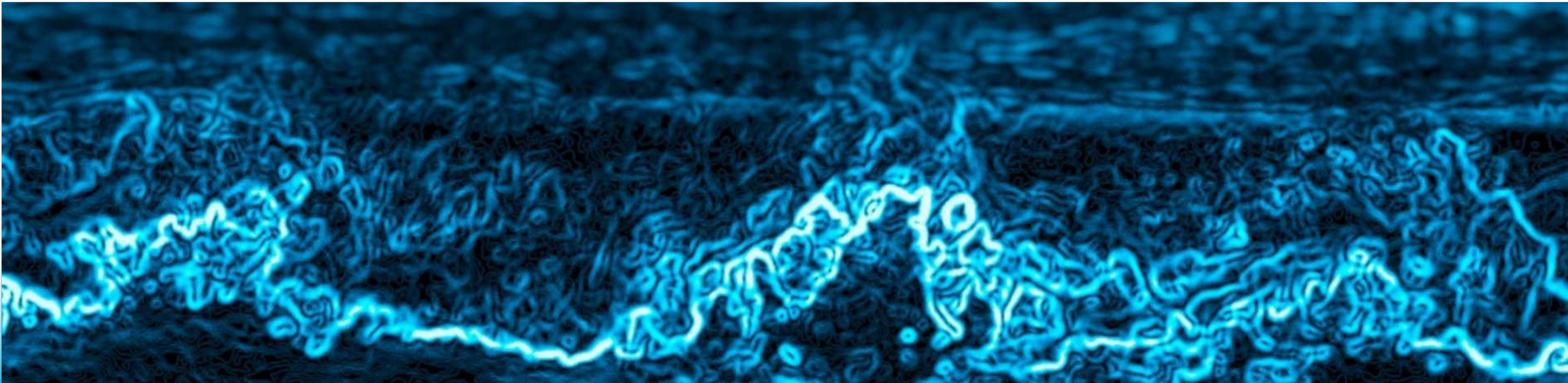




# IT STARTS WITH CYBER RESILIENCE

**Cyber Resilience** is a measure of your business ability to **continuously operate** and deliver on your intended outcome **despite adverse conditions**, stresses, attacks, or compromises.

**Cyber Resilience** exists when information security, business continuity, and organizational resilience are accomplished jointly.



# NIST Cybersecurity Framework

## Identify

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management Strategy

## Protect

Access Control

Awareness & Training

Data Security

Info Protection/  
Processes/Procedures

Maintenance

Protective Technology

## Detect

Anomalies & Events

Continuous Security  
Monitoring

Detection Process

## Respond

Response Planning

Communications

Analysis

Mitigation

Improvements

Cyber Insurance

## Recover

Recovery Planning

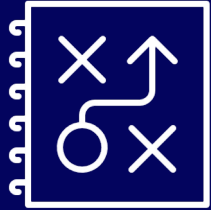
Improvements

Communications

Cyber Insurance







# Scenarios to Consider

## **An employee inadvertently...**

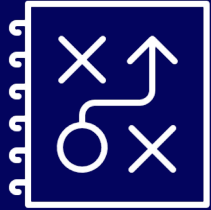
transmitted a virus to customers and suppliers. The company was sued for failing to contain the virus - losses totaled more than \$3,000,000.

## **An email that appeared to be from...**

a long-standing vendor relationship directed a company to update banking information for their account. The company paid over \$200,000 to the fraudster - no funds were recovered.

## **A hacker gained access to...**

the email account of an employee of a small accounting firm. The hacker used the email address to compromise several of the firm's client organizations - the firm was sued to the point of bankruptcy by their affected clients.



# Scenarios to Consider

## **Imagine if a hacker gained access to...**

the email account of a staff member with authority to direct other staff members, or communicate with client or partner.

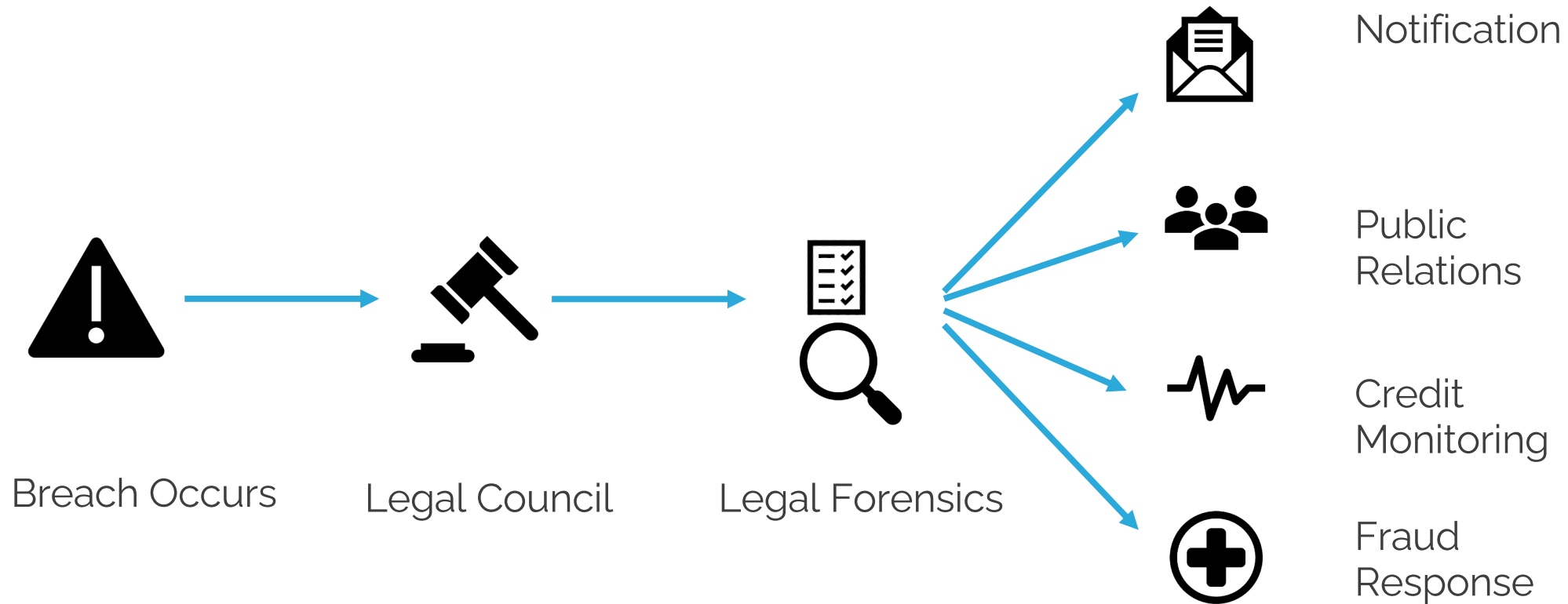
## **Imagine your reputational damage if...**

your connections to other partners or customers was exploited leading to their breach.

## **Imagine the disruption to your business...**

if all of your files and records disappeared suddenly and your systems used were inaccessible.

# CRISIS MANAGEMENT SERVICES





**Not All Cyber Insurance is created equal**

**Recommended Limits.**

Aggregate Limit	\$1,000,000
1st and 3rd Party Liability	\$1,000,000
Fines and Penalties	\$1,000,000
Fraud Response Expense	\$1,000,000
Public Relations Expense	\$1,000,000
Forensic Expense	\$1,000,000
Legal Expense	\$1,000,000
Notification Expense	\$1,000,000
Credit Monitoring	\$1,000,000
Extortion Loss/Ransomware	\$1,000,000
Business Interruption and Recovery	\$1,000,000
Multimedia & IP Liability	\$1,000,000
Reputational Damage	\$1,000,000
Data Replacement and Recovery	\$1,000,000
Hardware Replacement/Bricking	\$250,000 - \$1,000,000
Dependent Network Interruption	\$100,000 - \$1,000,000
Cryptojacking	\$100,000 - \$250,000
Invoice Manipulation	\$100,000 - \$250,000
Electronic Theft	\$250,000
Social Engineering	\$250,000
Telecommunications Theft	\$250,000

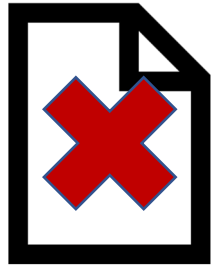
Full Aggregate Limit

Consistently sub-limited



# NOT ALL CYBER INSURANCE IS CREATED EQUAL

## No Coverage / Endorsement



- Added on to another line of coverage
- Limits are at or below \$100,000
- Probably never mentioned by their agent
- Low cost
- Not meant to pay claims
- Belongs in the garbage

## Stand-Alone Policy

Aggregate Limit	\$1,000,000
1st and 3rd Party Liability	\$1,000,000
Fines and Penalties	\$1,000,000
Fraud Response Expense	\$1,000,000
Public Relations Expense	\$1,000,000
Forensic Expense	\$1,000,000
Legal Expense	\$1,000,000
Notification Expense	\$1,000,000
Credit Monitoring	\$1,000,000
Extortion Loss/Ransomware	\$1,000,000
Business Interruption and Recovery	\$1,000,000
Multimedia & IP Liability	\$1,000,000
Reputational Damage	\$1,000,000
Data Replacement and Recovery	\$1,000,000
Hardware Replacement/Bricking	\$250,000 - \$1,000,000
Dependent Network Interruption	\$100,000 - \$1,000,000
Cryptolocking	\$100,000 - \$250,000
Invoice Manipulation	\$100,000 - \$250,000
Electronic Theft	\$250,000
Social Engineering	\$250,000
Telecommunications Theft	\$250,000

- All coverage are present
- Full limits, start at \$1M
- Designed to pay claims
- This is an investment
- Most likely had a specific conversation with their agent

# 5 MUST-HAVE SECURITY CONTROLS

When these controls are in place, this will increase a client's chance of obtaining an adequate insurance policy with the best rates.

1. Multi-Factor Authentication (MFA)
  - Remote access
2. Segregated Backups
3. Endpoint Detection and Response (EDR) and Next Gen Anti-Virus (NGAV)
4. Patching and Vulnerability Management
5. Cybersecurity Employee Training





## 5 MUST-HAVE SECURITY CONTROLS

Want to a better rate on your insurance? Add these:

1. Email filtering
2. 24x7 Managed EDR (usually mandatory for high risk businesses)
3. Local administrator rights removed for users and PAM tool in place
4. Formal vulnerability management





# HOW TO SPEAK “CYBER” INSURANCE



# THINGS YOU CAN AND CANNOT SAY

---

## OK to say

- Based on your size, most companies like you go for at least \$1MM in limits
- Here are the cybersecurity controls you need to address to be eligible for this policy

## NOT OK to say

- You need \$1M in coverage
- This policy is good for you
- You should choose this policy vs. the other one

# WHAT YOU NEED TO KNOW

- READ YOUR POLICY!
- Get in front of client policies at least 60 days in advance
- Understand Sub-limits
- Don't Be Afraid to Put a Carrier On Notice
- Get a Qualified Breach Coach / Attorney



# Common Client Objections



IT NATION™ **SECURE**



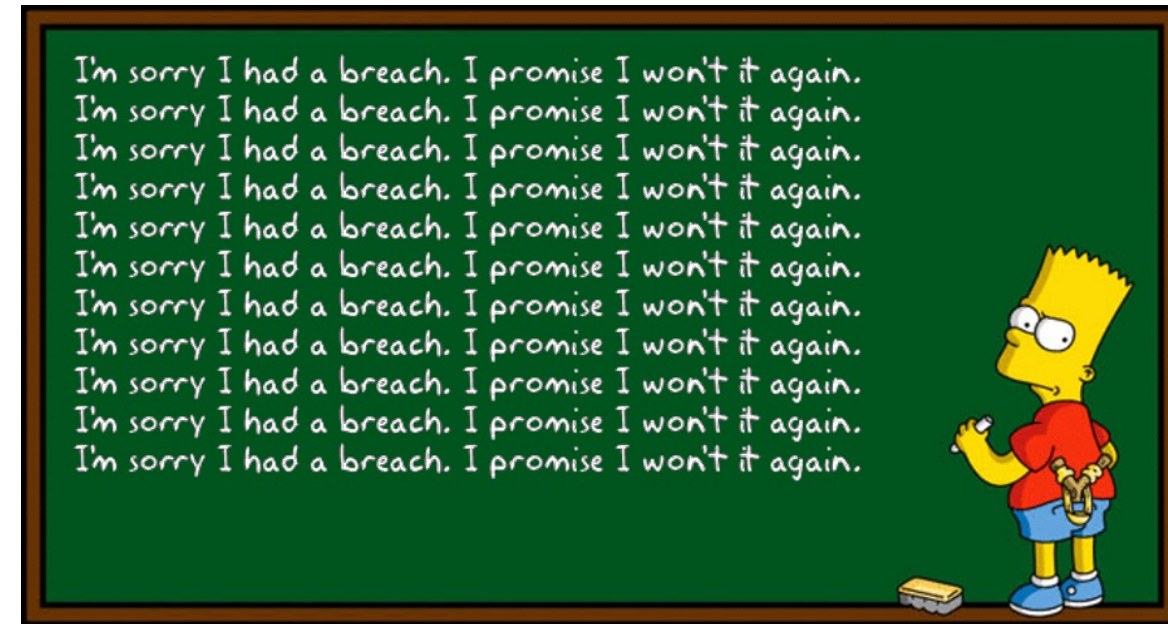
# “We have insurance but don’t need security, we’ll just file a claim”

Rates increasing 25%+ per *quarter*

- On average - companies with claims it is much more
- Or even worse – non-renewal!

Open claim = non-renewal

Security requirements going up for renewal each year



# Cyberinsurance does not pay out

“Endorsements” are the reason this myth exists

- Is the cyber part of another policy? Endorsement.
- Is the cyber policy a standalone policy? Not an endorsement – designed to pay out!
- Endorsements have no underwriting (i.e. security controls form)

Limits exist – know your policy!

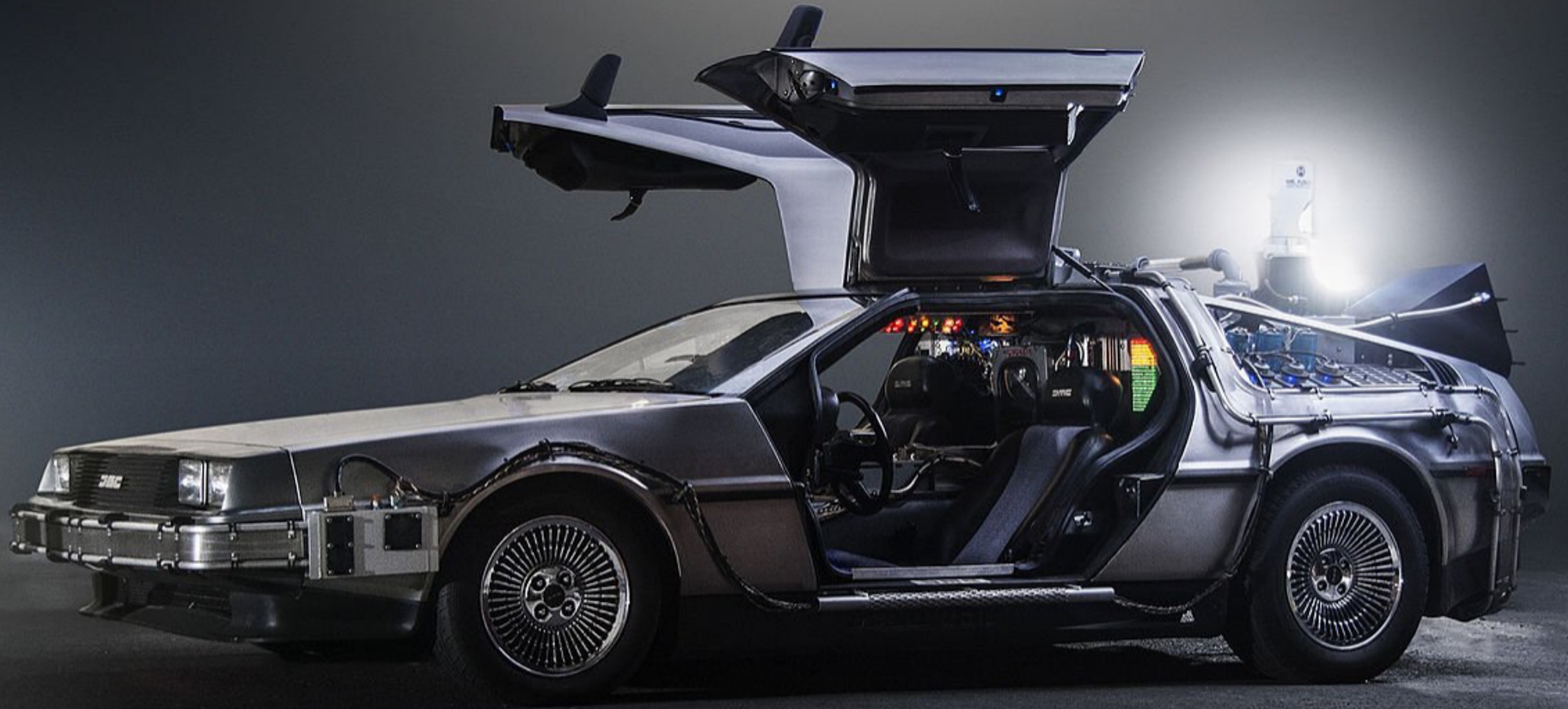
Bring in Fifthwall to explain and convince that an endorsement is not enough.

# We don't have sensitive data!

Every company has HR & payroll

Taking payments – what about PCI?

- Some apps are starting to ask about this, even what SAQ level you are



The future of cyber insurance



A man with long, flowing white hair is seated on the Iron Throne, a large, imposing chair constructed from dark, jagged blades. He is wearing a dark, heavy coat and has his hands clasped in his lap. The scene is set in a dimly lit room with a window in the background, through which some light is visible. The overall atmosphere is somber and dramatic.

**DATA**



SPEED  
LIMIT  
55









# HOW FIFTHWALL CAN HELP & NEXT STEPS

We'll ALWAYS review a policy for ANYONE for free

We're wide open to webinars talking about the state of cyber insurance and how you as a vendor help address insurance requirements

We're here just plain and simple to answer your questions and provide you feedback and data when you need it

---

**Don't assume** on cyber insurance. Find out exactly where your business stands.

**Learn more** at [fifthwallsolutions.com/msp](https://fifthwallsolutions.com/msp)

**Request a Policy Review** or Side-by-Side Comparison

#ITNation





# KEY TAKEAWAYS

The **quantity** of cyber attacks is **rising**; you must preemptively **plan** for a security event

Cyber insurance is key to **controlling your recovery costs**

Not all cyber policies are equal; make sure you **understand your coverage**

Get involved 2-3 months in **advance**

Insurance carriers are **raising their security expectations**

Failure to meet core controls may lead to **denied coverage or claims**

READY TO POWER UP?

SCAN ME



[EMPATHCYBER.COM/POWERUP](https://empathcyber.com/powerup)

JOIN OUR WEEKLY NEWSLETTER  
WITH THOUSANDS OF MSPS  
GROWING IN SECURITY!



# Thank you!

Follow me at:

- [CyberFOX.com](https://www.CyberFOX.com)
- [Empathcyber.com](https://www.Empathcyber.com)
- [Linkedin.com/in/wesspencer](https://www.linkedin.com/in/wesspencer)
- [Youtube.com/wesspencer](https://www.youtube.com/wesspencer)





*Don't forget to fill out your*

# **SESSION SURVEY**